A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

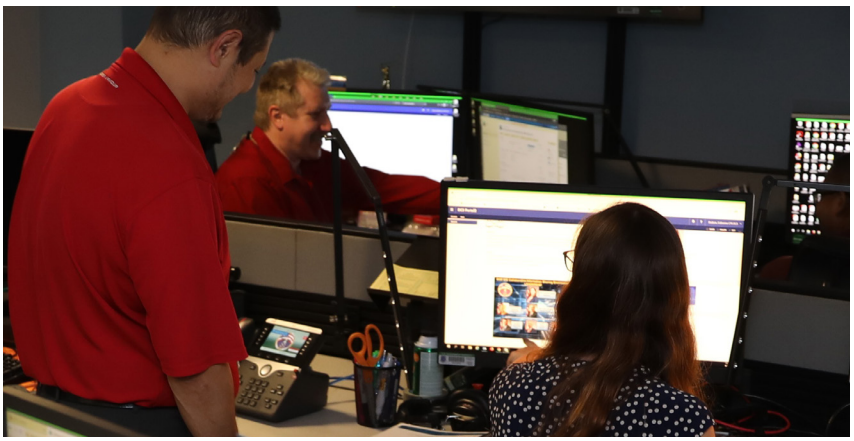
DoD—Defense Industrial Base Collaborative Information Sharing Environment

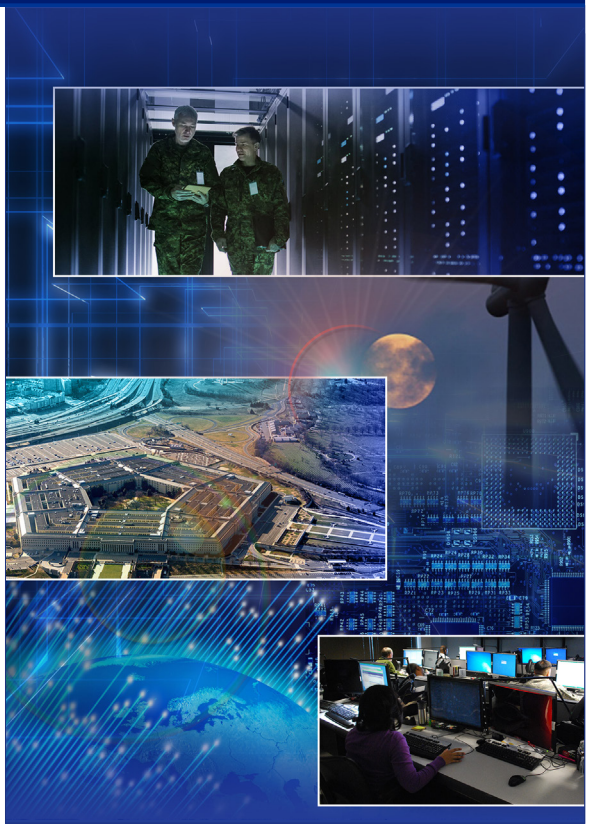
DCISE FACT SHEET

DoD-Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE)— DCISE is the operational hub for DoD's Defense Industrial Base (DIB) Cybersecurity Program, focused on protecting intellectual property and safeguarding DoD content residing on or transiting contractor unclassified networks. DCISE develops and shares actionable threat products, performs cyber analysis and diagnostics, and provides remediation consults for DIB partners.

DCISE is the reporting and analysis hub for the implementation of Section 941 of the Fiscal Year 2013 National Defense Authorization Act of certain types of cyber incidents by Cleared Defense Contractors (CDCs), and of the related amendment in the Defense Federal Acquisition Regulation Supplement (DFARS 252.204-7012). Cyber incidents outlined in DFARS are submitted to DCISE as mandatory reports; however, all other cyber incidents can be reported voluntarily.

- Rated at Maturity Level 3 under the Capability Maturity Model Integration for Services (CMMI-SVC)
- Collaborative partnership with over 700 CDCs and US Government (USG) agencies
- 442,000+ actionable, non-attributable (to submitting source) indicators
- 74,000+ hours of no-cost forensics and malware analysis for DIB Partners
- 13,000+ cyber threat reports





" The threat is real. By sharing our findings, we can reduce risk together. "

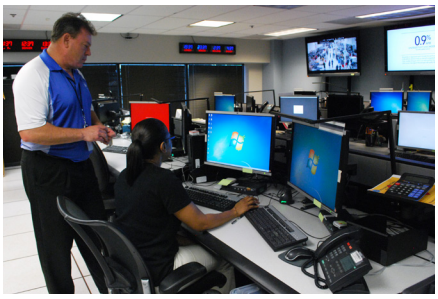
—DCISE

DoD CYBER CRIME CENTER

DCISE@dc3.mil 410-981-0104 | www.dc3.mil | info@dc3.mil

@DC3Forensics
@DC3 Cyber Crime Center

DCISE CAPABILITIES



Analytics Division (AD): AD conducts cyber analysis on information submitted by DIB Partners, the DoD and other USG-related reporting to provide a complete understanding of known or potential threats to unclassified DoD information on or transiting DIB systems and networks. AD also analyzes aggregate data from DIB Partner incident reports to produce technical analysis products, presentations, and white papers. The Division collaborates with liaison officers from other USG agencies to create and maintain both technical and multi-source threat profiles. Analytic tasks are broken into two branches:

1. **Tactical Operations:** Conducts daily functions related to processing of voluntary and mandatory incident reports as well as malware analysis, Customer Response Forms (CRFs), CRF Supplements, and Partner engagement.
2. **Applied Research:** Handles mid-to-long term analytic functions related to processing of Threat Activity Reports (TARs), Cyber Targeting Analysis Reports (CTARs), Alerts, Warnings, and other risk-based analyses. Works the downgrade and release of information derived from USG sources through Cyber Threat Bulletins (CTBs) and Threat Information Products (TIPs).

External Operations (XOP) Division: XOP researches services that can support DIB Partners in protecting DoD information. These services are offered as pilots to the DIB Partnership. The pilots range from services to technologies and are intended to encompass all concepts, technologies, and processes within cybersecurity. XOP was created because of the need for evolving solutions based on the ever changing cybersecurity environment and the diverse composition of the DIB partnership. Three branches constitute XOP:

1. **Assess Branch:** Performs analysis of cybersecurity processes of DIB partners through the Cyber Resilience Analysis (CRA) tool. This branch also evaluates other vulnerability and pen testing assessment procedures and provides them as a service to the DIB Partnership.
2. **Assist Branch:** Evaluates different cybersecurity technologies that can be provided to the DIB partnership as a pilot. Once the pilot is offered to the DIB, the information gathered from the capability is passed on to AD to determine if the information is applicable. Once the pilot is completed and if it is determined to be successful, it may be considered as a permanent service offering for the Partnership.
3. **Architect Branch:** Researches and identifies the most effective ways to communicate with the DIB partnership. Their research discovers technologies that can best support transmitting cyber threat information from AD to the Partnership.

Mission Support Division (MSD): MSD executes functional areas including internal/external customer services, outreach, operational metrics, process improvement, quality assurance, quality control, and organizational training. MSD builds and manages relationships with a wide range of DIB companies and USG stakeholders, and drives special projects that improve the overall customer experience. MSD is comprised of two branches:

1. **Customer Engagement:** Primarily responsible for customer relationships; DIB Partner on-boarding and outreach campaigns to promote DIB participation, as well as event planning for Technical Exchanges and Regional Partner Exchanges; and facilitating Analyst-to-Analyst and Business-to-Business Exchanges.
2. **Organizational Readiness:** A team of knowledge managers, business and process analysts, quality control analysts, quality assurance analysts, process owners, and support staff to drive continual process improvement. Systematically coordinates and aligns resources and functions with the DCISE vision, mission, goals, and objectives through the DCISE Performance Management Plan.